MARSH JLT SPECIALTY

INSIGHTS | ISSUE 46

Cyber Decoder

A US Supreme Court recently rejected an appeal by a US-based online retailer in a proposed data breach class action lawsuit. The appeal is seen as a setback for companies looking to limit their liability to data breaches.

The case centres on a 2012 data breach, in which customers' names, email addresses, phone numbers, and credit card information were compromised. At the time, the retailer took immediate action to mitigate the impact of the breach, notifying customers and asking them to change their passwords.

In the six years since the breach, only a very small number of the millions of affected customers have reported that their data had been misused. Despite few customers suffering concrete injury, the retailer faces a class action lawsuit.

Difficulty in proving injury should be a major hurdle in bringing legal actions in the US. However, cases such as this continue to push boundaries, as the plaintiff bar seeks ways to bring class actions for data breaches involving personal data.

Question of Harm

The company has the case hinged on whether customers affected by a data breach can sue a company, even if their data has not been misused and they have not suffered any real damage, such as identity theft or fraud.

Consumers affected by a data breach are required to demonstrate actual or impending harm in order to sue. However, in the case in question, the customers of the online retailer argued their personal information could theoretically be misused at any time.

A district court in Nevada previously found that customers that had suffered a financial loss had legal standing to sue, but the rest did not. However, a California-based federal appeals court reversed the district court's decision, saying customers could sue if they are able to show there is an impending substantial risk of harm.

US courts are divergent in their view of standing in data breach cases. Several US courts have adopted a plaintiff-friendly view, giving consumers legal standing on the basis of potential for future harm. Others, by contrast, have concluded that fear of future harm is too speculative to meet standing requirements.

It was hoped that this recent case might go before the Supreme Court, potentially resulting in a landmark decision on standing in data breach class actions to provide some much needed guidance. However, the Supreme Court denied the petition at the end of March 2019.

Contents

MARSH

GDPR

Data breach class actions are also an emerging trend in Europe, where the EU's General Data Protection Regulation (GDPR) has made it easier for consumers to seek compensation. In addition to increased privacy rights for consumers, the GDPR includes provisions for collective actions and allows affected individuals to seek compensation for non-financial damage, such as emotional distress.

A number of data breaches in the past year have sparked proposed class actions in the UK, against airlines, retailers and technology companies.

Even before the GDPR, a large UK supermarket retailer was sued following a data breach involving its employees' personal data. In October 2018, the Court of Appeal dismissed the retailer's attempt to overturn a previous ruling, which held the company vicariously liable for the actions of a former employee, who stole employee data and published it online.

The case - the UK's first data breach class action - also involved employees seeking compensation for a data breach, even though they had not suffered financial loss. In April, the retailer was granted permission to appeal to the UK's Supreme Court.

Open door

In many cases, individuals that have their personal data compromised in a data breach do not suffer significant financial loss, which has proved a hurdle to consumer-based data breach class action in the US. Companies that suffer a data breach typically would mitigate the impact through expedient notification and the provision of free services, like credit monitoring or identity theft protection. However, plaintiff attorneys continue to pursue data breach actions in the US.

The US Chamber of Commerce noted that data breach litigation, where personal information is accessed, but almost no identity theft or fraud has occurred, is increasingly common. It said a number of other companies face similar suits over alleged vulnerabilities in internet-connected cars, home security systems, children's toys and medical devices.

The Supreme Court's denial and recent appeal court ruling leaves the door open for expensive litigation against companies that experience a cyber security breach and suffer the loss of personal data. Even where a business takes reasonable steps to prevent a data breach and mitigates the impact when they do happen, they are open to costly litigation.

CCPA

The California Consumer Privacy Act, which comes into force on January 1, 2020, could also have implications for data breach litigation. According to law firm Hogen Lovells, the CCPA provides a limited private right of action for data breach suits. In certain circumstances, consumers may seek actual damages or statutory damages between US$100 and US$750 per incident, whichever is greater.

The law firm said the plaintiffs' bar is likely to argue that the CCPA's statutory damages provision dispenses with their obligation to show actual injury and particularised harm. In February, a bill was introduced to the California State Senate that would amend the CCPA to expand the private right of action. If the bill is passed as drafted, consumers would be able to file suit for any alleged violation of their CCPA rights, without any demonstration of harm, Hogen Lovells said.

Breach Costs and the Intensity of Cyber Attacks Rise

The introduction of tough EU data protection laws in May 2018 prompted some companies to bolster their cyber security. However, many companies have experienced an increase in cyber attacks and higher losses from data breaches, according to recent studies.

Rising Cost

Almost one third (32%) of businesses experienced a cyber security attack in the last 12 months, down from 43% the previous year, according to the 2019 Cyber Security Breaches Survey, published by the UK's Department for Digital, Culture, Media and Sport (DDCMS). The incidence of cyber attacks was, however, much higher among medium size businesses (60%) and large businesses (61%).

While fewer businesses have identified breaches or attacks, the ones that have are typically experiencing more of them. In addition, the cost of a data breach has risen significantly, according to the DDCMS report, which surveyed over 1,500 UK companies of varying sizes.

Of those businesses that suffered attacks, the median number of breaches rose from four in 2018 to six in 2019. The survey also shows that 48% of attacked businesses identified at least one breach or attack every month. The most common breaches or attacks were phishing emails, followed by instances of others impersonating their organisation online, viruses and other malware, including ransomware.

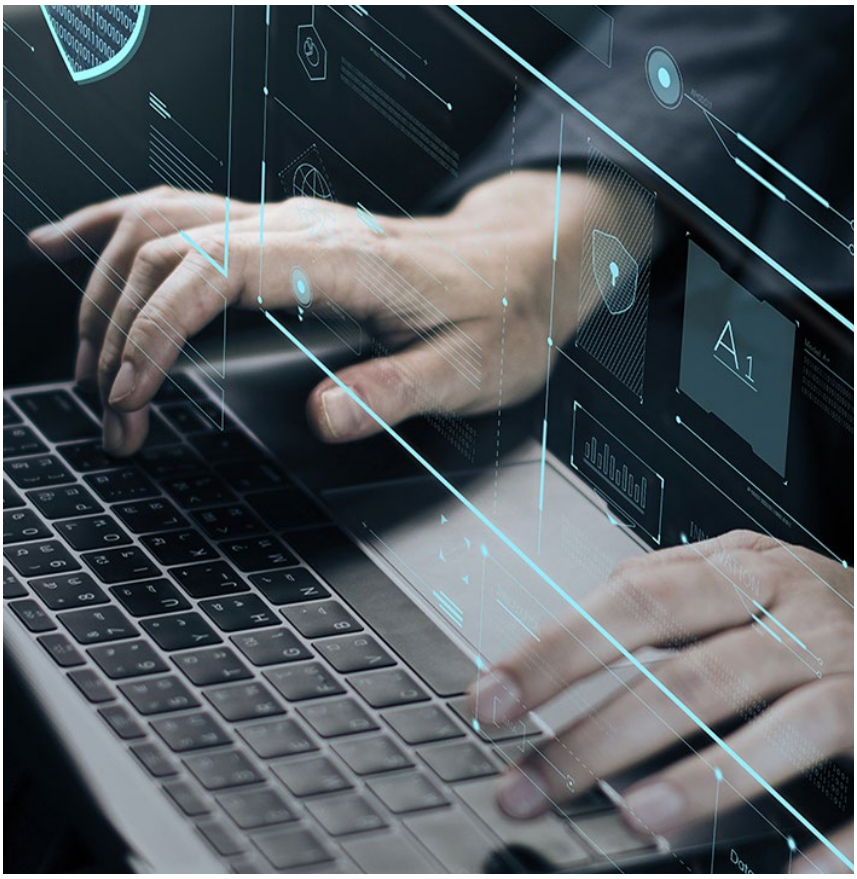
The average cost of a cyber attack for a business has increased by more than £1,000 since 2018 to £4,180. The average cost faced by larger businesses is typically much higher at £9,270 for medium size firms and £22,700 for large firms in 2019. For companies that suffered a breach, 19% said staff had been stopped from carrying out their daily work, while 27% said employees were diverted to deal with an attack.

However, companies often undervalue the true cost and impact of cyber security breaches, according to the report. Indirect costs, long-term costs and intangible costs of breaches, such as lost productivity or reputational damage, tend to be overlooked.

Greater Intensity

Another study by insurer Hiscox also reported a sharp increase in the cost of cyber attacks. Hiscox Cyber Readiness Report 2019, which surveyed more than 5,400 organisations across seven countries, found average losses associated with all cyber incidents increased 61% to US$369,000. For large firms cyber-related losses are now on average US$700,000, compared with US$162,000 a year ago.

Hiscox's report, which surveyed private and public sector organisations in the US, UK, Belgium, France, Germany, Spain and the Netherlands, also recorded an increased intensity of cyber attacks.



Three out of five firms (61%) experienced one or more attacks in the past year, up from 45% in the 2018 report.

The study also noted an increase in attacks against small and medium size firms. While larger firms are still the most likely to suffer a cyber-attack, the proportion of small firms reporting an incident was up from 33% to 47%. In contrast, the proportion among medium size firms leapt from 36% to 63%.

Interestingly, Hiscox also found that supply chain incidents are now commonplace. Nearly two-thirds of firms (65%) have experienced cyber-related issues in their supply chain in the past year, and just over half (54%) now evaluate the security of their supply chains at least once a quarter or on an ad hoc basis.

Encouraging Signs

The DDCMS survey found encouraging signs that business leaders are taking cyber security more seriously than ever before. For example, the survey found that a number of companies had increased their planning and defences against cyber attacks since 2018.

The number of companies with a written cyber security policy has increased – in 2019, 33% said they had such a policy, compared with 27% in 2018. A similar picture emerges with cyber risk assessments - in 2019, 31% said they had carried out a cyber risk assessment in the past 12 months, compared with 24% in 2018.

Another positive trend has been board engagement with cyber risk, although there is still some way to go, according to the report. The proportion of businesses with a board member dedicated to cyber security has increased by five percentage points since 2018 to 35% this year, and is much higher at 59% for large companies.

More businesses (57% in 2019 compared with 51% in 2018) update their senior management on actions taken around cyber security at least once a quarter. Over the longer term, the proportion of businesses saying they never update senior managers has fallen from 26% in 2016 to 17% in 2019.

GDPR Boost

The overall reduction in companies experiencing a cyber attack may be the result of tough new data protection laws under the General Data Protection Regulation (GDPR), according to DDCMS. Almost a third (30%) of businesses have made changes to their cyber security policies and processes as a result of the new rules, implemented in May 2018.

However, the reduction could also be down to a change in attacker behaviour, with more attacks focused on a narrower range of businesses, it said.

While the GDPR appears to have positively impacted cyber security, organisations need to think more "holistically" about the issue, the DDCMS said. The findings suggest that the GDPR has had some unintended consequences and led some organisations to frame cyber security largely in terms of exclusively avoiding personal data breaches.

To Do List

With the rising costs and intensity of attacks, the DDCMS concludes that businesses can no longer ignore the threat of cyber and should make cyber security and risk management a priority. There is more that organisations can do to protect themselves from cyber risks, according to DDCMS, particularly around board level involvement in cyber security, monitoring suppliers and planning incident response.

While more businesses now have a board member with specific responsibility for cyber security, the proportion remains low overall, according to the report. A similar picture emerges for monitoring suppliers and planning incident response - only one in five businesses (18%) require their suppliers to adhere to any cyber security standards, while just 16% have formal cyber security incident management processes in place.

Training is another area highlighted as having a "long way to go" to ensure organisations are better protected. Less than three in 10 (27%) of those companies have trained staff to deal with cyber threats in the last 12 months.

Like DDCMS, Hiscox also highlighted the need for organisations to improve their cyber security. Despite an increased threat from cyber, more companies failed cyber readiness tests, it said. Nearly three-quarters (74%) were ranked as unprepared, while only one achieved "expert" status in 2019, compared with 11% in 2018.

Cyber Insurance

The Hiscox survey also showed growth in cyber insurance. 41% of the companies surveyed said they have taken out cyber insurance in the past year, compared with 33% in 2018; while a further 30% plan to take out cover in the year ahead. More than half of larger firms now have cover, but only 27% of smaller firms are protected, the insurer said.

The DDCMS report found cyber insurance purchasing rose significantly for medium size businesses (up to 31% from 19% in 2018) and large businesses (up to 35% from 24% in 2018). However, just 11% of all businesses have a specific cyber security insurance policy, which goes almost unchanged since 2018.

Companies are of the view that the cyber insurance market has become more developed, with policies appearing to be more accessible than before, according to in-depth interviews with some survey respondents. Some respondents also said that insurance premiums had decreased.

Only 3% of organisations with cyber insurance said they had made a claim. However, a number of organisations said the main drivers for taking up insurance were breach response and crisis management services. They said these extras help manage the reputational damage from a breach, which was their greatest concern.

Some organisations were also found to be using cyber insurance as a proxy form of accreditation. Having insurance was something they could advertise to their business clients to demonstrate they had undertaken due diligence, the report said.

New Cyber Supply Chain Threat Detected

A new supply chain attack has emerged in recent months, which has brought this growing and hard to detect cyber threat to the forefront.

In March, Kaspersky Lab revealed that hackers had compromised the systems of a major Taiwanese computer manufacturer and pushed out a malicious update signed with a legitimate digital certificate to customers. According to the cyber security firm, the attack affected at least 57,000 computers, but the total could be as high as one million users worldwide.

Dubbed, ShadowHammer, the newly discovered supply chain attack is since thought to have affected other companies. Kaspersky Lab found evidence that ShadowHammer has targeted six other organisations, including a number of Asia-based gaming companies, IT service providers and a pharmaceutical company. Hackers compromised the systems of these companies in order to target their customers through altered source code or injected malware.

Growing vulnerability

Supply chain attacks are a hot topic, following the compromise of managed service providers (MSPs) and several software products in recent years. According to cyber security firm Symantec, supply chain attacks have increased 78% over the past year.

Supply chain cyber attacks use legitimate software, IT services or third party app developers to deliver malware or malicious software code to target companies, which in turn can be used by hackers to steal data or gain control of IT systems. Such attacks can be hard to detect and enable hackers to breach multiple companies at once.

Hacking group Magecart, for example, is thought to be targeting third-party services to get its code onto targeted websites. The group was behind a number of large data breaches in 2018, including some high profile credit card skimming attacks against the consumer facing websites of an airline and online ticket vendor. In the latter, Magecart compromised a third-party chatbot, inserting malicious code into the web browsers of consumers visiting the website in a bid to steal their payment data.

In 2017, hackers targeted a small software company and inserted malicious code into a legitimate PC clean up tool. The incident reportedly affected over two million downloads, by both individuals and businesses, and resulted in further attacks against large technology and telecommunications companies in the UK, Taiwan, Japan, Germany and the US.

NotPetya, the global malware attack that caused worldwide disruption in June 2017, was also an example of a supply chain attack. Attackers managed to introduce malware into MeDoc, a legitimate software application widely used by businesses in Ukraine for handling tax returns. The compromised MeDoc update infected users of the application, while the malware spread itself within networks.

Cyber espionage group Dragonfly (also known as Energetic Bear) is thought to have targeted energy companies through their industrial control systems (ICS) software supply chains. This included hacking ICS software suppliers to replace legitimate files in their repositories with malware infected versions. In essence, the malware "trojanised" legitimate ICS software. When the ICS software was downloaded from suppliers' websites, it installed malware alongside legitimate ICS software, enabling hackers to gain remote access to the target company systems.

Supply Chain Cover

It is important for an organisation to consider the impact of a cyber attack on its technology and IT supply chain, including having an understanding of third party suppliers and their cyber security, as well as concentrations of risk and interdependencies.

Companies are often reliant on a small number of major software, hardware and service providers, meaning one attack could potentially affect a large number of companies within their supply chain. For example, a major US software provider, which provides services to 400,000 organisations worldwide and 98% of the Fortune 500, revealed in March that it was investigating a cyber attack after the FBI had warned the company that it may have been targeted by hackers.

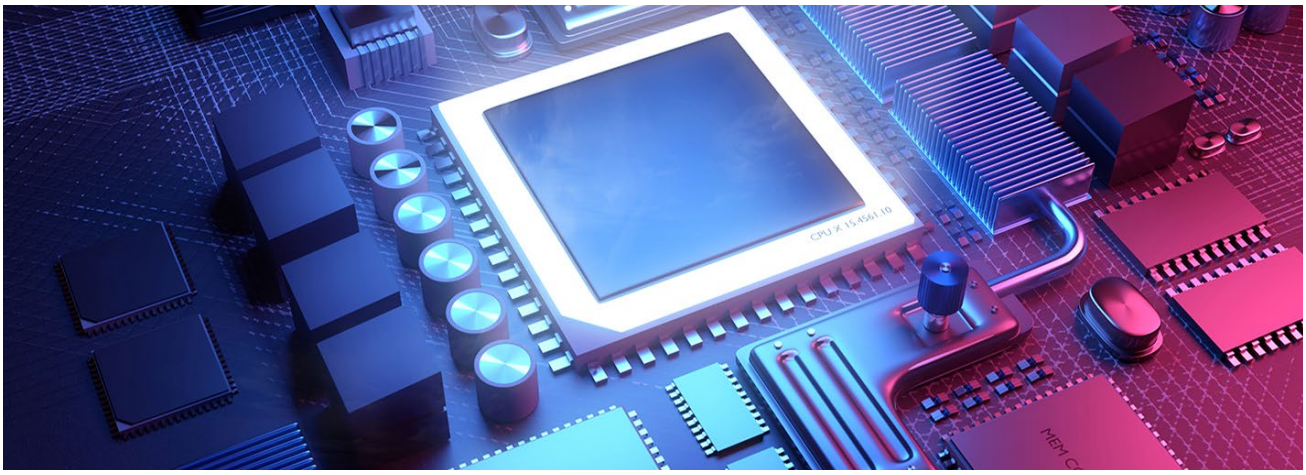
Insurance cover for cyber attacks within the technology and IT supply chain is widely available. Companies are advised to discuss this issue with their broker and check appropriate cover is included in their cyber insurance policy.

New Laws to Strengthen Data Protection Have Had a Positive Impact on Cyber Security

More than half of British firms "report cyber attacks in 2019", according to Hiscox. The insurer found that 55% of companies had faced an attack in 2019, up from 40% last year. But almost three quarters of firms were ranked as "novices" in terms of cyber readiness. Hiscox said a lot of businesses "incorrectly felt that they weren't at risk".

The firm surveyed more than 5,400 small, medium and large businesses across seven countries, including the UK, Germany, the US, Belgium, France, the Netherlands and Spain. It reported a "sharp increase" in the number of cyber attacks this year, with more than 60% of firms having reported one or more attacks - up from 45% in 2018. Average losses from breaches also soared from US$229,000 (£176,000) to US$369,000, an increase of 61%.

A report from Beazley revealed a 133% increase in business email compromise incidents from 2017 to 2018. Beazley also found that the average ransomware demand in 2018 was more than US$116,000, but this was skewed by some very large demands. The median was US$10,310. The highest demand received by a Beazley client was for US$8.5 million – the equivalent of 3,000 Bitcoin at the time. Small-to-medium size businesses, which tend to spend less on information security, were at a higher risk of being hit by ransomware than larger firms.



Upcoming Events

2019 Advisen Cyber Risk Insights Conference

16 May 2019, Chicago

Event addressing the critical privacy, network security, and cyber insurance issues confronting risk professionals and their organisations; Elisabeth Case, Head of Cyber Advisory at Marsh moderates a panel on The Buyer's Perspective: Setting the Scene for Cyber Success.

Insurance Journal Cyber Webinar

21 May 2019

Marsh West Zone Cyber Leader, Florence Levy speaks on free webinar by leading insurance industry publication, focusing on cyber insurance – trends, value, challenges, and direction.

Find out more

Fast Forward: The Future of Insurance

23 May 2019, Romania

A full-day conference with top industry experts and European policy makers about the future of insurance in a changing world with ever increasing risks (e.g. natural catastrophes; cyber risk).

Find out more

Net Diligence Cyber Risk Summit

13 June 2019, Philadelphia

At this annual Philadelphia conference, Bob Parisi, Marsh US Cyber Product Leader, will speak on a panel about cyber and non-cyber: getting coverage right.

Find out more

SEACEN Policy Summit

13-14 June 2019, Malaysia

A discussion with the Central Bank Leadership in combating cyber risk. Naureen Rasul, Asia Cyber Practice Leader at Marsh (Hong Kong) Limited will be presenting amongst others.

Intro to Cyber Programme

13 June 2019

Running Concurrently with the main NetDiligence cyber summit, a special morning session developed for future insurance, legal and technical security professionals. George Holevas, Vice President from the FinPro Practice at Marsh will be speaking at this event.

IBC's Cyber Insurance APAC 2019

2-3 July 2019, Singapore

A broker's perspective on market development trends and emerging products. Naureen Rasul, Asia Cyber Practice Leader at Marsh (Hong Kong) Limited will be presenting amongst others.

URMIA Annual Conference

19 September 2019, Boston

At the University Risk Management and Insurance Association's 50th annual conference, Marty Leicht, North East Zone Leader, speaks on panel about navigating the current cyber risk insurance market landscape: gaps and overlaps.

AFP 2019

22/23 October 2019, Boston

At the annual conference of the Association for Financial Professionals, Marsh will co-lead a panel on proactive strategies to combat payment fraud.

Find out more

Cyber Buying Trends Highlighted in Asia Survey

Pre-acquisition, JLT Asia put together a regional survey on the latest Cyber buying trends across Asia in January 2019. 2018 saw cyber security issues dominating headlines across Asia and a continued uptake in cyber insurance, with a 50% increase in JLT Asia's policy count and a 70% increase in the total premium placed in the insurance market.

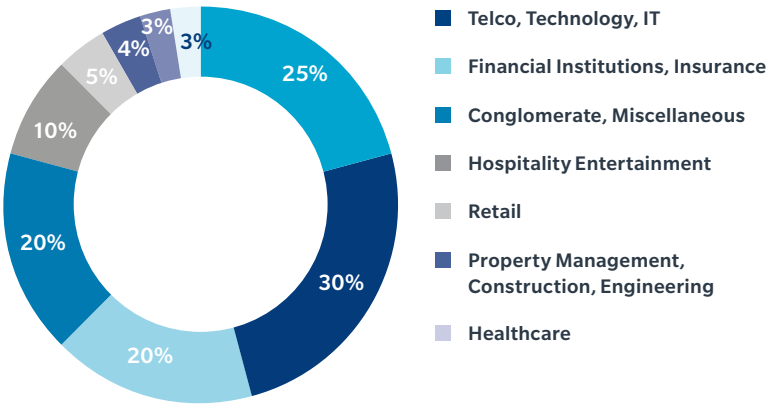
Below are the key cyber buying trends of 2018 noted in our regional survey, plus our predictions for 2019:

Cyber Insurance by Industry

Our survey found that Asian buyers of cyber insurance, consistent with the global market, are overwhelmingly in industries that rely heavily on technology and/or hold significant amounts of personal data. The technology and telecommunications sector made up 30% of our book over the past year; while Financial Institutions represented 20%. In addition, their reliance on operational technology (OT) exposes them to greater risk of business interruption from non-physical damage risks.

Despite the sensitive information risk, the Healthcare sector continues to only see a modest uptake in cyber insurance (3% of the book). However, the various high profile data breaches that caused significant financial impact within the Singaporean health sector in late 2018 may prompt a change of heart in 2019.

FIGURE 1 The following chart shows the percentage of cyber buyers by sector based on JLT Asia's 2018 book:



Limits and Cover

During 2018, average limits increased from US$6 million (2017) to US$8 million, while average premiums have increased by 20% year on year. This increase in limits and premium reflects a growing awareness of the product and its key role in protecting company balance sheets, as claims become increasingly frequent and severe.

Last year there was also a noticeable increase in companies purchasing non-physical damage business interruption cover prompted by all the cyber-attack publicity. Asian businesses continually stress that business interruption cover is a greater selling point of cyber insurance than data liability cover. According to the survey, 72% of our clients bought business interruption (BI) extensions in 2018, compared with just 62% in 2017. However, despite this increased uptake, insurers remain cautious about retention thresholds and there wasn't a substantial reduction in either monetary or waiting time retentions for BI cover.

Claim Notifications

We saw a steady increase in the number of claims present on our books in 2018, with the top three claims triggers being ransomware, privacy breach and network security breach. 40% of claim notifications came from Hong Kong in Asia and notifications were made under 12% of our policies.

2019 Predictions

We expect cyber uptake to continue to grow in the midst of new regulatory changes within the region, specifically in Singapore, China and the Philippines. The extra territorial reach of the EU's General Data Protection Regulation (GDPR) is also increasing the liability risk landscape, with business interruption being the most prominent concern.

In an attempt to address the unexpected silent cyber losses within the insurance market, we're starting to see more and more insurers looking to impose cyber "clarifications" under other insurance lines including; Property and Casualty (P/C), Professional Indemnity (PI) and Directors and Officers (D&O) Liability. These moves need to be carefully evaluated, as the potential implications for such a new risk area cannot be fully understood.

Debunking the Top 5 Ransomware Myths

By Cyber Collective Partner Winston Krone, Global Managing Director of Kivu Consulting.

When it comes to ransomware attacks, the general consensus of opinion is one of fear and confusion surrounding the appropriate steps to take once your systems have been disconnected and you receive a ransom demand. Winston Krone from cyber security firm Kivu Consulting provides some clarity on the subject and eliminates popular ransomware misconceptions one by one:

MYTH 1: 'HACKERS WON'T PROVIDE THE DECRYPTION TOOLS AND YOU'LL BE RIPPED OFF'

The majority of ransomware actors want to make money and receive good publicity within the hacker community on the Dark Web. When a hacker doesn't decrypt a system post-payment, it destroys their reputation within the community and lowers the chances of future ransoms being paid, so it is in their best interest to deliver on their promise. In some cases, the decryption software doesn't work properly and expert advice is needed.

Victims tend to panic and blame the attacker, but in practice it is rare for an attacker to deliberately fail to provide a fully functional decryption key. Often the hacker is inexperienced and turns to Ransomware as a Service (RaaS) tools to learn how to plan a ransomware attack, but when things go wrong, they don't know how to decrypt the data properly.

While the likelihood of an attacker not providing decryption keys is low, it's important to consider how that risk fluctuates depending on whether the victim wants to negotiate instead of paying the stated sum.

For example, when a victim is attacked by an aggressive variant and the victim attempts to substantially discount the initial ransom amount, attackers are more likely to "stiff" the victim and simply end all negotiations. It's worth remembering that attackers frequently carry out specific reconnaissance on the target's size and financial value, and they generate their perception of a "reasonable" ransom demand based on those metrics.

Often, an attacker has multiple victims and will respond first (or only) to the victims who provide the least resistance. Also, while paying the stated demand (or a slightly reduced counteroffer) usually results in successful acquisition of the decryption tool; we've also seen attackers initially accepting the terms of a surprisingly low counteroffer, only to turn around and demand the remaining funds following payment.

MYTH 2: 'ALL SERVERS ARE COMPATIBLE WITH DECRYPTION SOFTWARE'

New strains of ransomware are constantly being developed and tweaked to get around antivirus software. This rapid evolution has sped up the encryption process, but made the decryption process a lot slower (sometimes taking weeks), which frustrates companies. We've seen this first hand with the Ryuk and BitPaymer ransomware variants.

Rushing to get new variants on the market, criminal malware developers are only testing their code on the most common, modern computer systems. This makes victims with older servers and out-of-date operating systems particularly vulnerable to attack and subsequent destruction.

For example, Microsoft announced in July 2015 that it will no longer be supporting Windows 2003 and consumers were warned that older servers would not be adequately patched or protected anymore. When unpatched older systems get encrypted, they are typically destroyed and all the data they hold gets deleted.

This problem is exacerbated by unskilled attackers who launch a ransomware attack without the knowledge to shut down databases or log out of virtual machines pre-launch. Failure to do this guarantees system crashes and irreparable corruption, regardless of whether decryption keys are provided. This destruction is not something hackers want to happen, as it affects them being paid and means that the affected companies endure irreversible loss of their data.

Companies still operating on older systems are not regularly tested and will therefore find it harder to get comprehensive coverage for the inevitable loss of their files during an

attack. They should seek specialist advice to assess their options for cyber protection. Ensuring that servers are up-to-date and compatible with the latest strains of malware will make the decryption process a lot easier and less risky for data protection.

MYTH 3: 'THERE ARE OTHER WAYS TO CRACK THE ENCRYPTION'

There are lots of paid online adverts for special remedies to CrySis and Dharma ransomware, which involve paying outside agencies to decrypt a system without having to pay a ransom to the hacker. However, most of these tools simply don't work and slow the process down, costing more in the long run.

There is a lot of false information on the internet, which can prove detrimental. There are also unscrupulous vendors who will accept payment from a victim to decrypt a system, and then buy the decryption keys from the attacker. The victim then misleadingly believes that, having recovered its data without paying a ransom, it doesn't need to notify authorities about the event or take regulatory compliance actions.

For the most part, ransomware variants, for which legitimate free solutions exist, are now no longer in circulation. Ransomware actors typically avoid using variants that are widely known to be "decryptable". However, there are a few exceptions in the form of earlier versions of GandCrab. GandCrab remains one of the most effective and prevalent ransomware variants (especially the new versions), even though there are legitimate, free decryption tools for versions 1, 4 and some flavours of 5.

MYTH 4: 'RANSOM PAYMENT IS THE MOST CRUCIAL STEP'

Actually, the most difficult and integral part of the process is the decryption stage. Depending on the ransomware variant and the maturity of the victim's operating systems, the time required to decrypt can be substantial. If the environment is large, victims may not discover all encrypted machines until days or weeks later, which may warrant additional engagement with the bad actor and follow-up ransom payments.

Victims usually assume that receiving the decryption key is an immediate solution and don't prepare for the business interruption costs incurred while decryption is taking place.

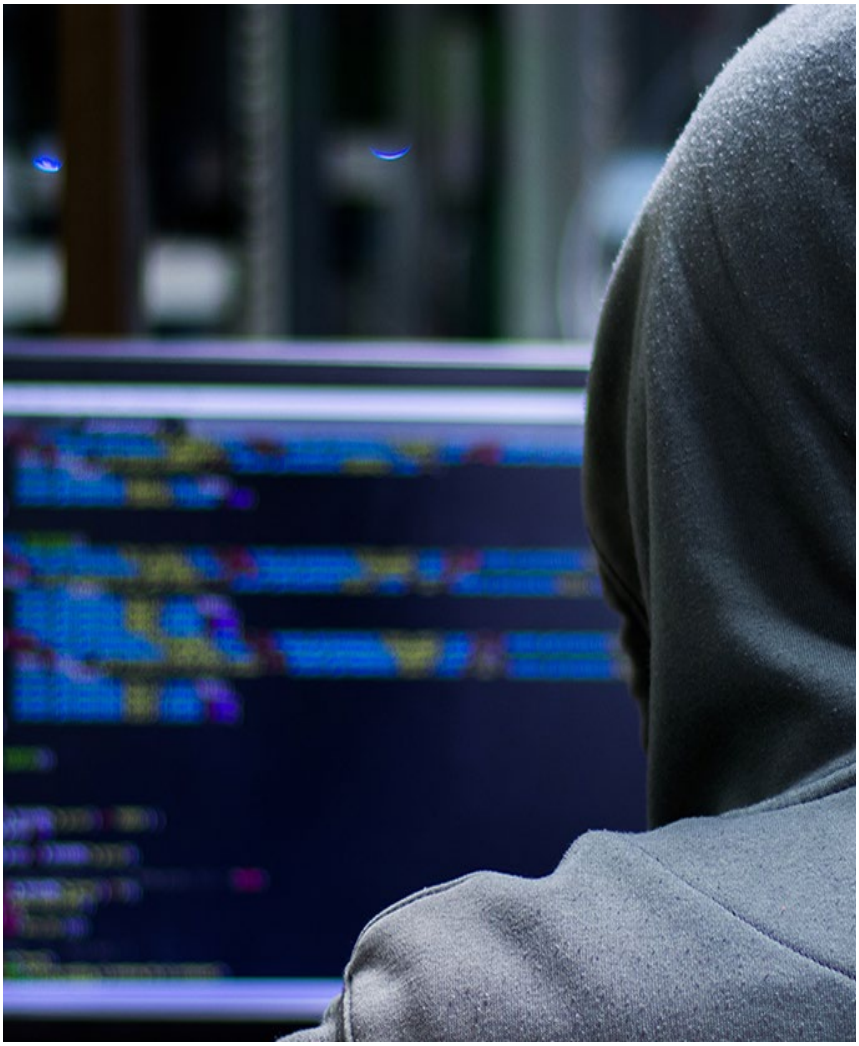
MYTH 5: 'CYBER CRIMINALS ONLY TARGET COMPANIES THAT HOLD A LOT OF PERSONAL DATA'

This assumption leads some companies to underestimate their level of risk and stops them from adequately preparing for an attack. The reality is that victims are chosen for their level of system vulnerability, not because of the amount or type of data they hold.

Consistent regulation, bigger security budgets and an enlightened C-suite who have thought more about the risks their companies face are the biggest differentiating factors between a prepared company and a vulnerable one. Although some attacks may be motivated by the size of the ransom companies can afford to pay, most victims are chosen because of their system vulnerabilities regardless of their size and budget.

Conclusion

No company, regardless of sector or size, is immune to a ransomware invasion if they continue to overlook their responsibility for robust cyber security. Having a clear cyber-attack strategy will put a company one step ahead of hackers and allow time for informed decision making amidst the chaos of a system lock out. Ultimately, a company's attitude towards their level of risk and their likeliness to engage with an incident response plan makes all the difference.



Quantification Adds Up to Better Cyber Risk Management

Managing cyber risk means different things to different people within an organisation. To the chief financial officer, it means building an insurance programme. To the chief information security officer, it means implementing technology and protocols. To the general counsel, it means complying with myriad regulations.

Yet with technology ingrained in virtually every business function, cyber exposures and vulnerabilities have multiplied. To effectively manage cyber risk, those stakeholders need to engage each other across internal boundaries. Bringing all of those stakeholders together, however, can be challenging. That's where cyber risk quantification can help.

A Lingua Franca

Despite the clear consensus that cyber represents a significant risk for businesses, many companies have yet to calculate the potential financial impact of a cyber event. Moreover, individual managers typically see only the risk aspects relevant to their function and they often each speak a different "language."

Quantifying cyber risk allows you to express cyber risk in a language common to all business stakeholders: economics. Equally important, quantification allows organisations to frame cyber in the same terms as other business risks and evaluate risk management investments on the same financial basis.

Data-Based Investment Decisions

Beyond providing a common method of expression, quantification allows a business to better understand the size of its risk: Is our value at risk US$10 million, or US$100 million? And it enables prioritisation of those risks: Is our biggest vulnerability data breach, technology interruption, or regulatory liability?

While qualitative terms like "high," "medium," or "low" are imprecise, quantitative modeling produces objective and actionable data to guide capital allocation decisions. Knowing the range of potential losses and areas of maximum risk enables better decision-making relative to your organisation's risk tolerance and capital allocation, including how much insurance coverage to buy, how to direct investments in cyber security technology and training, plus more.

Oversight and Transparency

A quantitative approach can also create a foundation for improved management of other critical cyber risk management functions, such as regulatory compliance. The Securities and Exchange Commission (SEC) outlined new requirements in 2018 for public companies to quantify and disclose their cyber security risks, report material cyber events, and outline their boards' role in cyber risk oversight.

Savvy investors — including institutional investors and fund managers — have come to view cyber security as an essential component in their analysis and valuation and thus now want the same information. To that end, they are seeking to understand the potential effect of cyber events on financial performance and market value. This means that responsibility for cyber risk disclosures must move from the investor relations function to the boardroom — yet another reason to use cyber quantification to broaden internal discussions.

As the cost of cyber events continues to rise, businesses are seeking better methods to prioritise and evaluate their risk investments. Uninformed spending is no longer acceptable. Instead, businesses should measure and evaluate cyber risk in financial terms, just as they do with other critical risks that can make or break their bottom lines.

Buzzword of the month

Evil Maid Attack

What Does it Mean?

Evil Maid attacks, named by Joanna Rutkowska, refer to scenarios that affect device integrity. This includes gaining unauthorised physical access to an unattended device with the purpose of changing, stealing or selling the information found on the device; and hackers selling 'brand new' laptops containing pre-loaded keyloggers or malware to unsuspecting victims.

Although the opportunities for this type of attack are limited, physical attacks can have a profound impact on the company. Skilled Evil Maids are able to bypass the login credentials and encryption of most corporate laptops within 30 seconds, so all it takes is for an employee or member of the C-suite to be distracted for a minute for them to gain access to your sensitive data.

The main targets of these sophisticated attacks are company executives, government officials and journalists, as their devices are the most likely to contain valuable data.

A typical Evil Maid attack goes as follows:

1. The Evil Maid will boot up the unattended device from a compromised bootloader (USB). They can also bypass security systems by installing malware onto the device or by simply typing in the password captured on hidden cameras within the room.
2. The attacker then installs a keylogger, which records the encryption key once entered on the device, and shuts the computer down. The encryption key can either be sent to the hacker via the internet or stored in a hidden location for retrieval.
3. Once the owner has unlocked the hardware, the Evil Maid can revisit the device to retrieve the keylogger, which now contains the encryption key. During this visit the Evil Maid will remove all traces of their interference. Alternatively, they can replace the device with an identical copy without the victim's knowledge.
4. The hacker is now free to remotely access all of the device's data.

Why Does it Matter?

In this emerging era of collaboration among hackers, firmware rootkits are now readily accessible for amateur hackers on the Dark Web for ease of access, thus increasing the likelihood of attack.

Most devices were not designed with physical security built in, but a variety of apps that are able to notify users when their devices are being physically accessed now exist.

Other ways an individual can reduce their chances of being attacked by an Evil Maid include:

- Never leaving devices and USBs unattended.
- Shutting down devices after use.
- Avoiding unknown USBs and hard drives.
- Ensuring that patch updates are applied without delay.
- Enabling input-output memory management unit (IOMMU) features.
- Enforcing secure boot protection and changing encryption keys regularly.
- Using strong passwords and changing them often.
- Enabling multi-factor authentication.
- Only booting the system from the hard drive.
- Setting up alerts and passwords for hardware changes.
- Using burner devices when travelling in high risk areas where attacks are commonplace.

For further information, please contact your local Marsh JLT Specialty office or visit our website at jlt.com.

SARAH STEPHENS
Head of Cyber/Technology E&O
Marsh JLT Specialty
cyber@jltgroup.com

Marsh JLT Specialty
The St Botolph Building
138 Houndsditch
London EC3A 7AW

Tel: +44 (0)20 7528 4444

www.jlt.com

 May 2019 • 280256